

Implementacja ukrytych funkcji w sposób utrudniający ich wykrycie

mgr inż. Paweł Koszut

Implementacja ukrytych funkcji

- Przykładowy system – opis
- Ukryta funkcja – sposób zaimplementowania

Opis systemu

Opis systemu

The screenshot shows an Internet Explorer browser window with the title "Internet Explorer Multiple Code Execution Vulnerabilities - Advisories - Secunia - Konqueror". The address bar shows the URL "http://secunia.com/advisories/28036/". The page content is organized into several sections:

- Solutions For:** Links for Security Professionals and Security Vendors.
- Free Solutions For:** Links for Open Communities and Journalists & Media.
- Software Inspectors:** Links for Scan Online, Personal (PSI), and Network (NSI).
- Secunia Advisories:** Links for Search, Historic Advisories, Listed By Product, Listed By Vendor, Statistics / Graphs, Secunia Research, Report Vulnerability, and About Advisories.
- Virus Information:** Links for Chronological List, Last 10 Virus Alerts, and About Virus Information.

The main content area is titled "Internet Explorer Multiple Code Execution Vulnerabilities" and includes the following details:

- Secunia Advisory:** SA28036
- Release Date:** 2007-12-11
- Last Update:** 2007-12-13
- Critical:** Indicated by a 4-bar green progress bar and the text "Extremely critical".
- Impact:** System access
- Where:** From remote
- Solution Status:** Vendor Patch
- Software:** Microsoft Internet Explorer 5.01, Microsoft Internet Explorer 6.x, and Microsoft Internet Explorer 7.x.
- CVE reference:** CVE-2007-3902, CVE-2007-3903, CVE-2007-5344, and CVE-2007-5347 (all with Secunia mirror links).

A section titled "Want to know the next time vulnerabilities are fixed in this product?" includes a link: "- Companies can be alerted via email and SMS!".

The **Description:** states: "Some vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system."

A numbered list starts with: "1) A use-after-free error in mshtml.dll when handling 'setExpression()' method calls can be".

On the right side of the page, there is a "The Secunia PSI - Technology Preview" advertisement with a "Download BETA" button. Below it is a "Secunia Poll" asking if the organization has taken extraordinary steps to remediate the Microsoft Windows URI vulnerability, with radio button options for Yes, No, and No, we're not affected. A "Vote!" button and a "See Results" link are also present. At the bottom right, there is a "Most Popular Advisories" section listing "1. Microsoft Windows" with a 4-bar green progress bar.

Opis systemu

The screenshot shows an Internet Explorer browser window with the title "Internet Explorer Multiple Code Execution Vulnerabilities - Advisories - Secunia - Konqueror". The address bar shows the URL "http://secunia.com/advisories/28036/". The page content is organized into several sections:

- Solutions For:** Links to "Security Professionals" and "Security Vendors".
- Free Solutions For:** Links to "Open Communities" and "Journalists & Media".
- Software Inspectors:** Links to "Scan Online", "Personal (PSI)", and "Network (NSI)".
- Secunia Advisories:** Links to "Search", "Historic Advisories", "Listed By Product", "Listed By Vendor", "Statistics / Graphs", "Secunia Research", "Report Vulnerability", and "About Advisories".
- Virus Information:** Links to "Chronological List", "Last 10 Virus Alerts", and "About Virus Information".

The main content area displays the following details for the "Internet Explorer Multiple Code Execution Vulnerabilities":

- Secunia Advisory:** SA28036
- Release Date:** 2007-12-11
- Last Update:** 2007-12-13
- Critical:** Represented by a 5-color bar (green, yellow, orange, red, dark red) and labeled "Extremely critical".
- Impact:** System access
- Where:** From remote
- Solution Status:** Vendor Patch
- Software:** [Microsoft Internet Explorer 5.01](#), [Microsoft Internet Explorer 6.x](#), and [Microsoft Internet Explorer 7.x](#)
- CVE reference:** [CVE-2007-3902](#) (Secunia mirror), [CVE-2007-3903](#) (Secunia mirror), [CVE-2007-5344](#) (Secunia mirror), and [CVE-2007-5347](#) (Secunia mirror)

There is a section titled "Want to know the next time vulnerabilities are fixed in this product?" with a sub-link: "- [Companies can be alerted via email and SMS!](#)".

The "Description" section states: "Some vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system." A numbered list item 1) reads: "A use-after-free error in mshtml.dll when handling 'setExpression()' method calls can be".

On the right side of the page, there is a "The Secunia PSI - Technology Preview" advertisement with a "Download BETA" button. Below it is a "Secunia Poll" asking: "Have your organisation taken any extraordinary steps to remediate the [Microsoft Windows URI](#) vulnerability?" with radio button options: "Yes", "No", and "No, we're not affected". A "Vote!" button and a "See Results" link are also present.

At the bottom right, there is a "Most Popular Advisories" section with a 5-color bar and a list item 1. The system tray at the bottom shows the time as 11:00 and the date as 12/11/2007.

Opis systemu

The screenshot shows an Internet Explorer browser window with the following content:

- Browser Title:** Internet Explorer Multiple Code Execution Vulnerabilities - Advisories - Secunia - Konqueror
- Address Bar:** http://secunia.com/advisories/28036/
- Navigation Sidebar (Left):**
 - Solutions For:** [Security Professionals](#), [Security Vendors](#)
 - Free Solutions For:** [Open Communities](#), [Journalists & Media](#)
 - Software Inspectors:** [Scan Online](#), [Personal \(PSI\)](#), [Network \(NSI\)](#)
 - Secunia Advisories:** [Search](#), [Historic Advisories](#), [Listed By Product](#), [Listed By Vendor](#), [Statistics / Graphs](#), [Secunia Research](#), [Report Vulnerability](#), [About Advisories](#)
 - Virus Information:** [Chronological List](#), [Last 10 Virus Alerts](#), [About Virus Information](#)
- Main Content Area:**
 - Internet Explorer Multiple Code Execution Vulnerabilities** (with Danish and German flags)
 - Secunia Advisory:** SA28036
 - Release Date:** 2007-12-11
 - Last Update:** 2007-12-13
 - Critical:** [Extremely critical](#)
 - Impact:** System access
 - Where:** From remote
 - Solution Status:** Vendor Patch
 - Software:** [Microsoft Internet Explorer 5.01](#), [Microsoft Internet Explorer 6.x](#), [Microsoft Internet Explorer 7.x](#)
 - CVE reference:** [CVE-2007-3902](#) (Secunia mirror), [CVE-2007-3903](#) (Secunia mirror), [CVE-2007-5344](#) (Secunia mirror), [CVE-2007-5347](#) (Secunia mirror)
 - Want to know the next time vulnerabilities are fixed in this product?**
- [Companies can be alerted via email and SMS!](#)
 - Description:** Some vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system.
 - 1) A use-after-free error in mshtml.dll when handling "setExpression()" method calls can be**
- Right Sidebar:**
 - The Secunia PSI - Technology Preview** (with a small screenshot of the PSI interface)
 - Download BETA**
 - Secunia Poll:** Have your organisation taken any extraordinary steps to remediate the [Microsoft Windows URI](#) vulnerability?
 Yes
 No
 No, we're not affected
[See Results](#)
 - Most Popular Advisories:** 1. [Microsoft Windows](#)

Opis systemu

Internet Explorer Multiple Code Execution Vulnerabilities - Advisories - Secunia - Konqueror

Location Edit View Bookmarks Tools Settings Help

http://secunia.com/advisories/28036/ Google Search

Internet Explorer Multiple ... Internet Explorer Multiple ...

Solutions For

- [Security Professionals](#)
- [Security Vendors](#)

Free Solutions For

- [Open Communities](#)
- [Journalists & Media](#)

Software Inspectors



- [Scan Online](#)
- [Personal \(PSI\)](#)
- [Network \(NSI\)](#)

Secunia Advisories


- [Search](#)
- [Historic Advisories](#)
- [Listed By Product](#)
- [Listed By Vendor](#)
- [Statistics / Graphs](#)
- [Secunia Research](#)
- [Report Vulnerability](#)
- [About Advisories](#)

Virus Information

- [Chronological List](#)
- [Last 10 Virus Alerts](#)
- [About Virus Information](#)

Internet Explorer Multiple Code Execution Vulnerabilities  

Secunia Advisory: SA28036
Release Date: 2007-12-11
Last Update: 2007-12-13

Critical:  [Extremely critical](#)

Impact: System access
Where: From remote
Solution Status: Vendor Patch

Software: [Microsoft Internet Explorer 5.01](#)
[Microsoft Internet Explorer 6.x](#)
[Microsoft Internet Explorer 7.x](#)

CVE reference: [CVE-2007-3902](#) (Secunia mirror)
[CVE-2007-3903](#) (Secunia mirror)
[CVE-2007-5344](#) (Secunia mirror)
[CVE-2007-5347](#) (Secunia mirror)

Want to know the next time vulnerabilities are fixed in this product?
- [Companies can be alerted via email and SMS!](#)


Data Loss Prevention
Learn more about Proofpoint's data loss prevention & email security
[www.proofpoint.com](#)

firewall security
Firewall Log Analysis for Security, Traffic, and Bandwidth Management
[www.FWAnalyzer.com/FreeTrial](#)

Description:
Some vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

1) A use-after-free error in mshtml.dll when handling "setExpression()" method calls can be

The Secunia PSI
- Technology Preview



Download BETA


Secunia Poll

Have your organisation taken any extraordinary steps to remediate the [Microsoft Windows URI](#) vulnerability?

Yes
 No
 No, we're not affected

[See Results](#)

Most Popular Advisories

1. 

Opis systemu

The screenshot shows the xfdiff application window. The title bar reads "xfdiff". The menu bar includes "File", "Diff Settings", "Patch Settings", "Actions", and "Help". The left pane shows the file "c8054f0f4178a37af0c1626232eb8f2f_54.html" and the right pane shows "c8054f0f4178a37af0c1626232eb8f2f_55.html". A green checkmark and "Apply" button are visible between the panes. The diff view shows HTML code with several lines highlighted in red, indicating differences between the two files. The status bar at the bottom contains buttons for "Clear", "Down", "Up", "Next file", "Previous file", and "Quit".

```
<td style="padding:4px"><br class="SGodstep">
<table border="0" cellspacing="4" cellpadding="2">

<tr valign="top">
<td>
<a href="gid,9490872,statp,Zm90b3RlbWF0TGldGFHYWxlcmpl,fototemat.html"><img src=152 152
<td width="100%"><div style="overflow:hidden; width:70px;"><a href="gid,9490872,statp153 153
</tr>

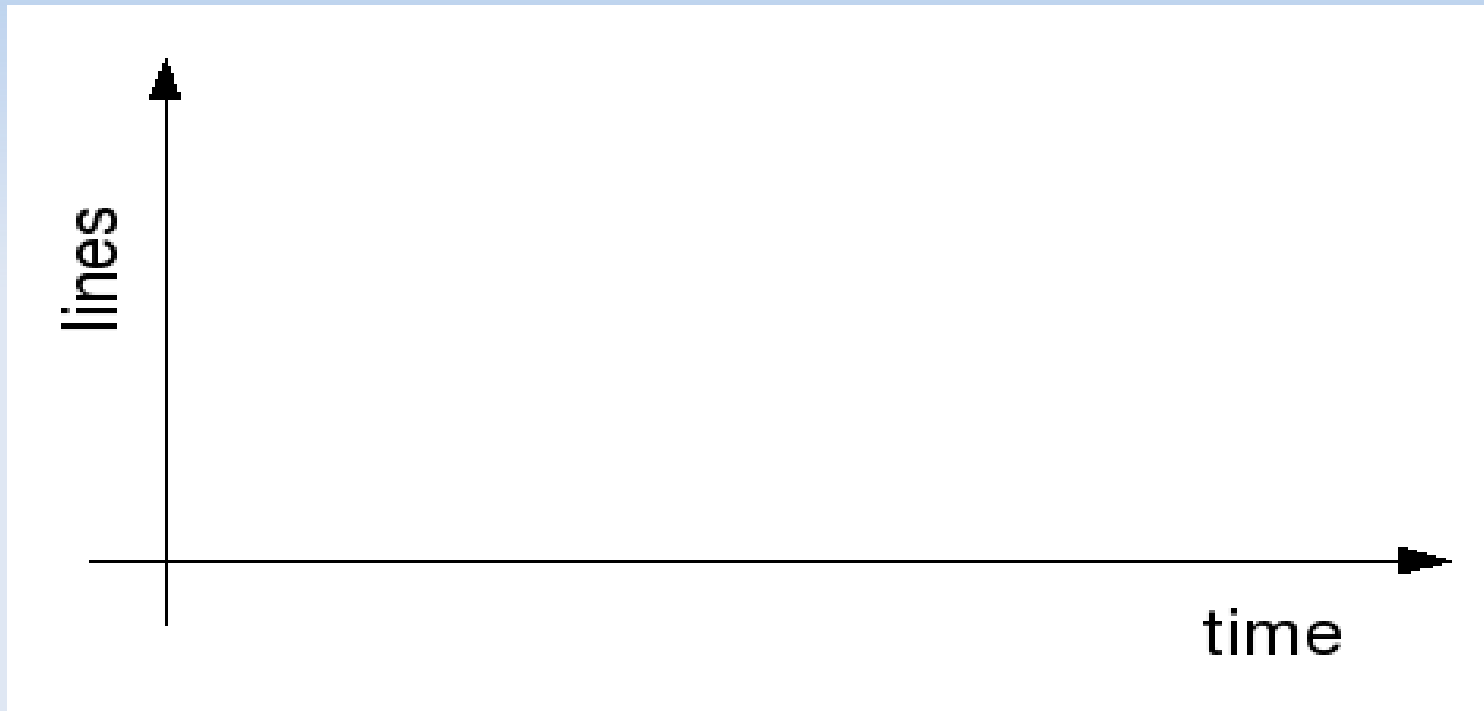
<tr valign="top">
<td>
<a href="gid,9490233,statp,Zm90b3RlbWF0TGldGFHYWxlcmpl,fototemat.html"><img src=159 159
<td width="100%"><div style="overflow:hidden; width:70px;"><a href="gid,9490233,statp160 160
</tr>

<tr valign="top">
<td>
<a href="gid,9490196,statp,Zm90b3RlbWF0TGldGFHYWxlcmpl,fototemat.html"><img src166 166
<td width="100%"><div style="overflow:hidden; width:70px;"><a href="gid,9490196,statp167 167
</tr>
</table>

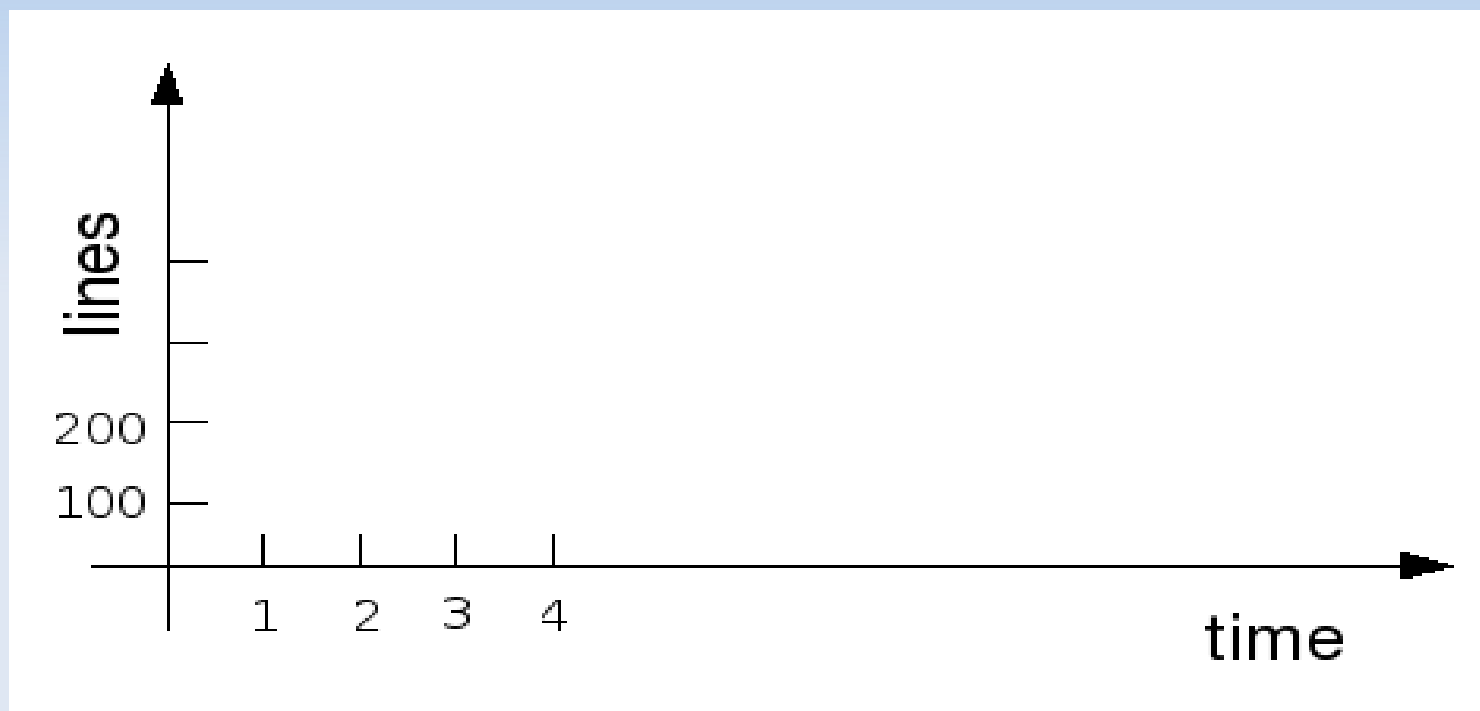
<div id="tylkowp">
<br />
<div class="content">
<table width="98%" cellpadding="0" cellspacing="0" border="0"><tr><td style="pa
<div class="dotLi">
<a href="/gid,9486331,kat,21114,statp,dHlsa29XV1A%3D,galeriazdjecie.html">
```

Working diff...
xfdiff> Different block: -36,7 +36,7
xfdiff> Showing difference number 1
xfdiff> Different block: -55,7 +55,7
xfdiff> Different block: -138,7 +138,7
xfdiff> Different block: -148,22 +148,22
xfdiff> Different block: -367,17 +367,17
xfdiff> Different block: -466,7 +466,7
xfdiff> *** Total of 7 different sections found

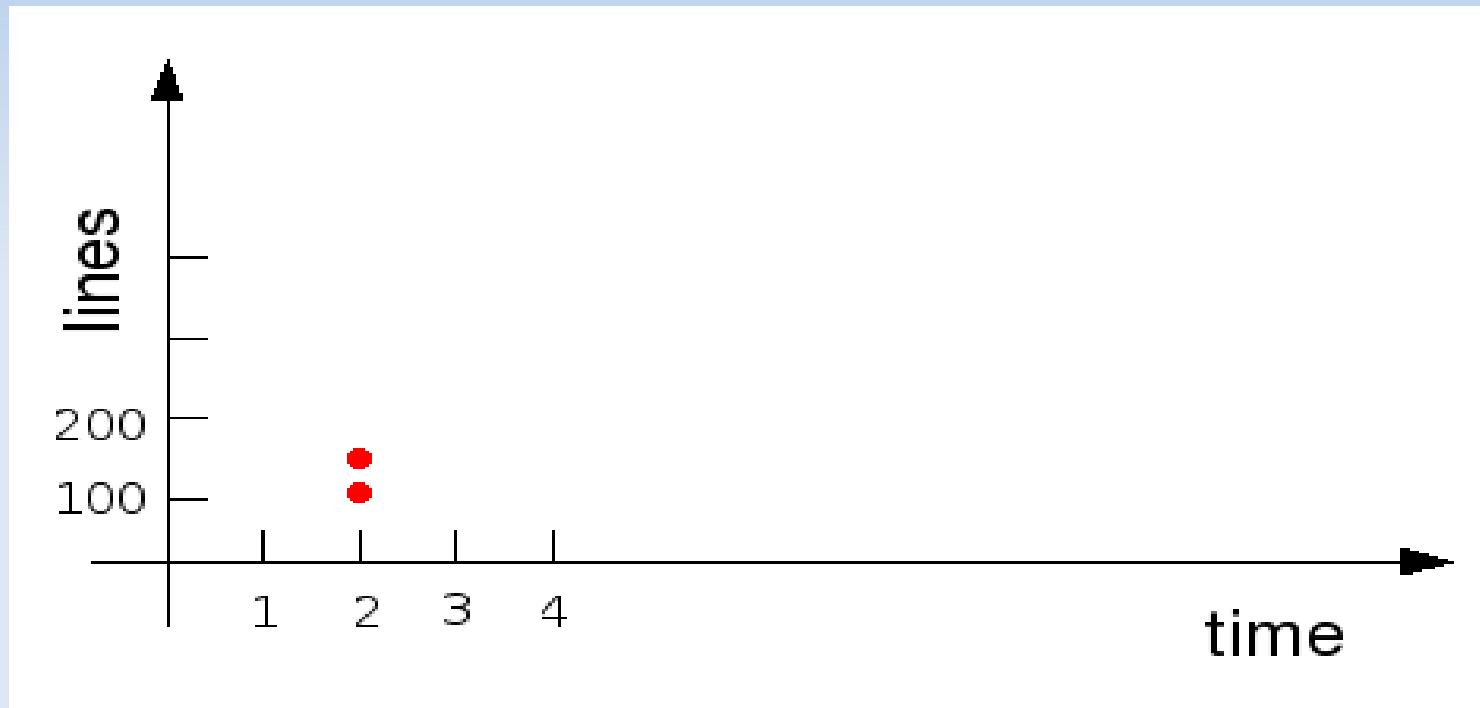
Opis systemu



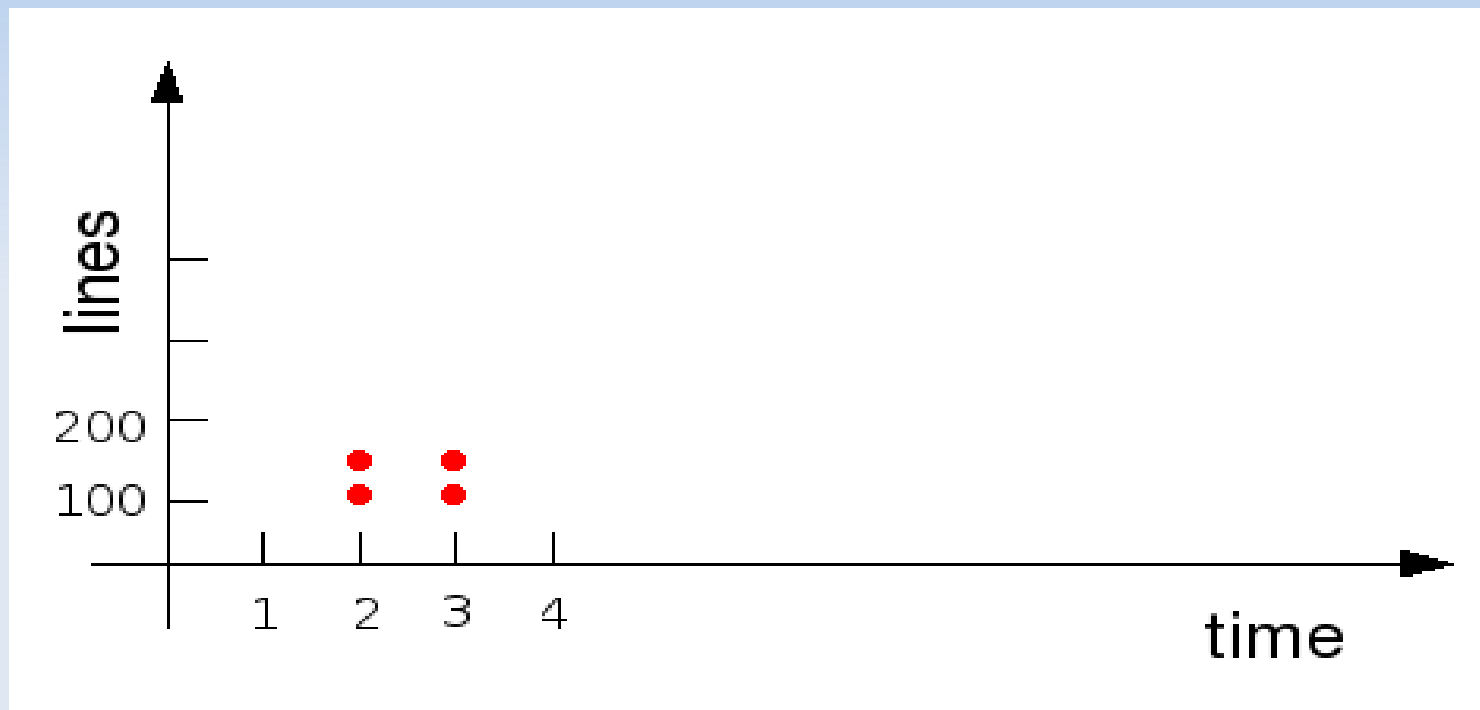
Opis systemu



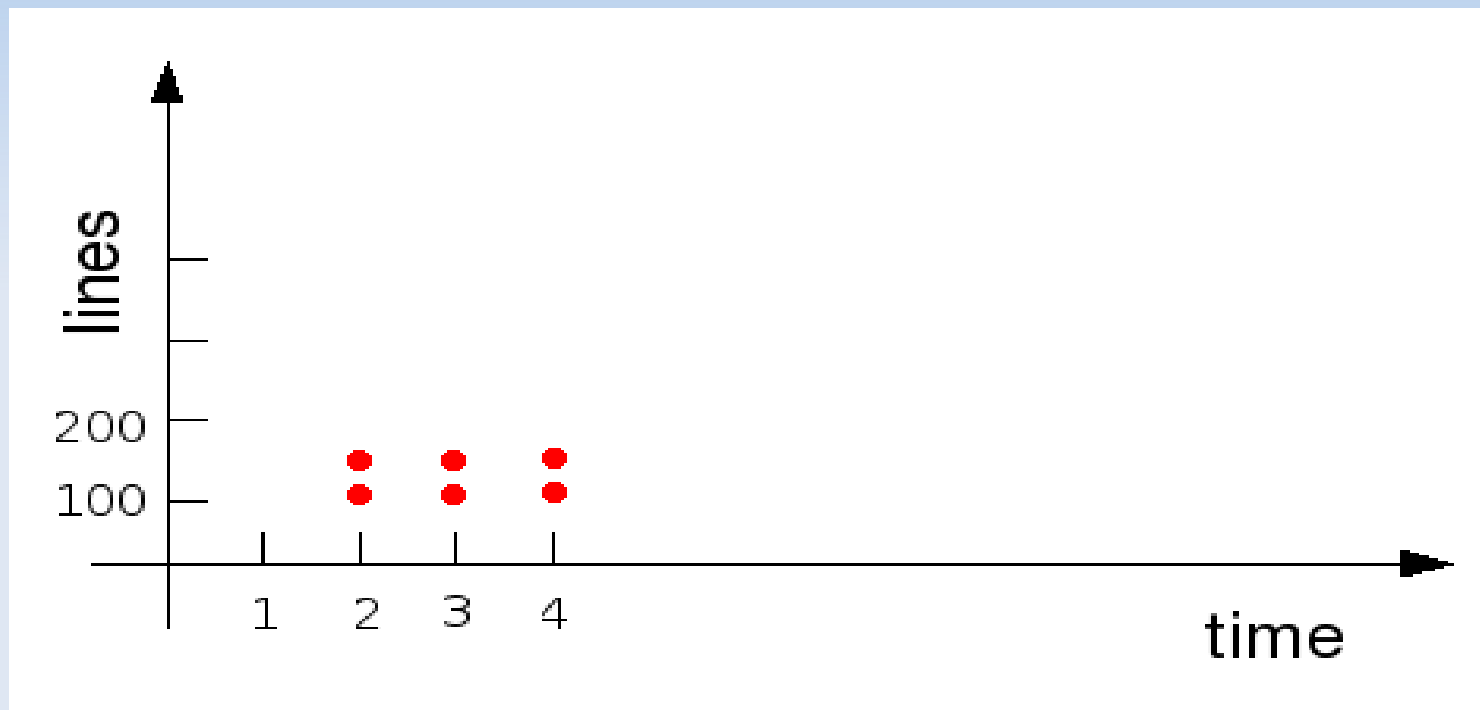
Opis systemu



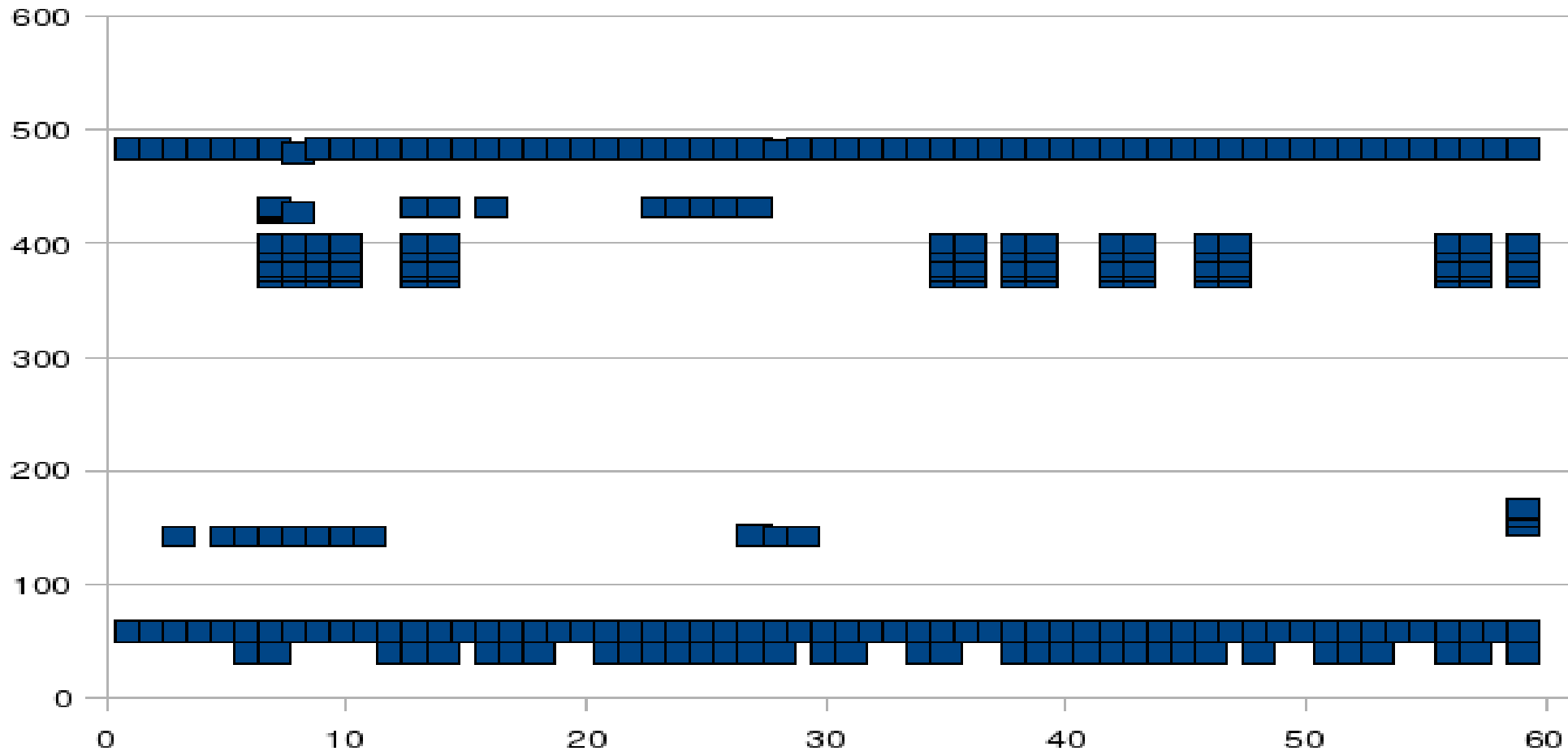
Opis systemu



Opis systemu



Opis systemu



Opis systemu

BBC NEWS | Business | Iraqi oil exceeds pre-war output - Konqueror

Location Edit View Bookmarks Tools Settings Help

Google Search

BBC NEWS | Business | Iraqi...

UK version International version

BBC NEWS

WATCH One-Minute World News

Accessibility help


News services
Your news when you want it

News Front Page

Last Updated: Friday, 14 December 2007, 17:31 GMT

[E-mail this to a friend](#) [Printable version](#)

Iraqi oil exceeds pre-war output
Iraqi oil production is above the levels seen before the US-led invasion of the country in 2003, according to the International Energy Agency (IEA).



Iraq's oil infrastructure appears to be getting back on track

The IEA said Iraqi crude production is now running at 2.3 million barrels per day, compared with 1.9 million barrels at the start of this year.

It puts the rise down to the improving security situation in Iraq, especially in the north of the country.

But the IEA warned that attacks on Iraqi oil facilities remain a threat.

In southern Iraq, more than 85% of the residents of Basra believe British troops have had a negative effect on the Iraqi province since 2003, according to a BBC poll.

The survey for BBC Newsnight of nearly 1,000 people also suggests that 56% believe their presence has increased the overall level of militia violence.

Sabotage attacks

In its latest monthly Oil Market Report, the IEA puts the Iraqi

THE STRUGGLE FOR IRAQ

KEY STORIES

- [Zawahiri says UK 'fleeing Basra'](#)
- [UK troops return Basra to Iraqis](#)
- [Iraqi oil exceeds pre-war output](#)
- [US marine guilty of Iraq killing](#)
- [US Senate passes Iraq funds bill](#)
- [Basra residents blame UK troops](#)
- [Triple car bombs hit south Iraq](#)

BACKGROUND AND ANALYSIS

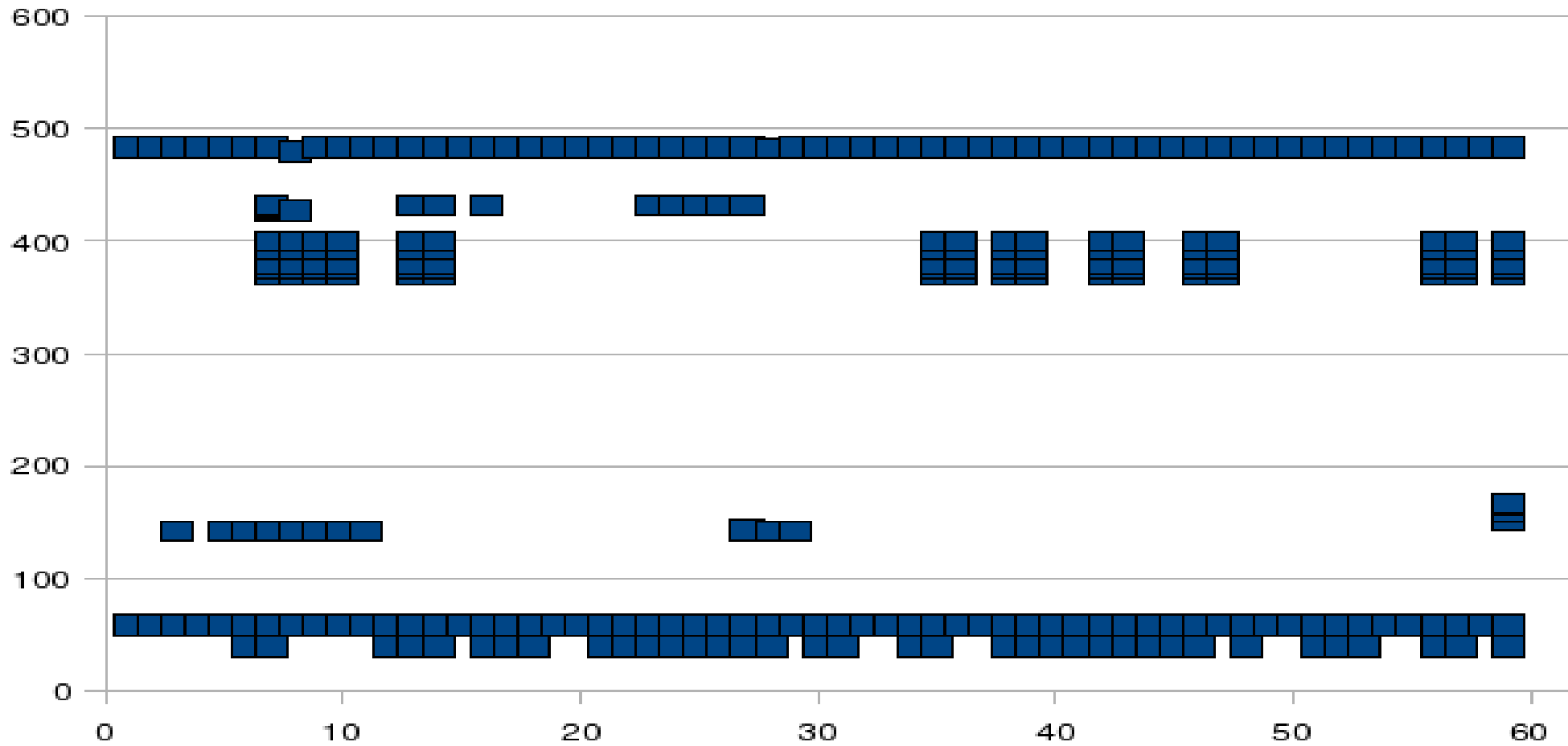
- [Basra uncertainty](#)
- [The future for the city as British troops hand over control](#)
- [Basra's new era](#)
- [Heading back home to Iraq](#)
- [Sunni 'neighbourhood watch'](#)
- [Political delay on death row](#)
- [Is Iraq getting better?](#)
- [Iraq violence in figures](#)

ANDREW NORTH DIARY

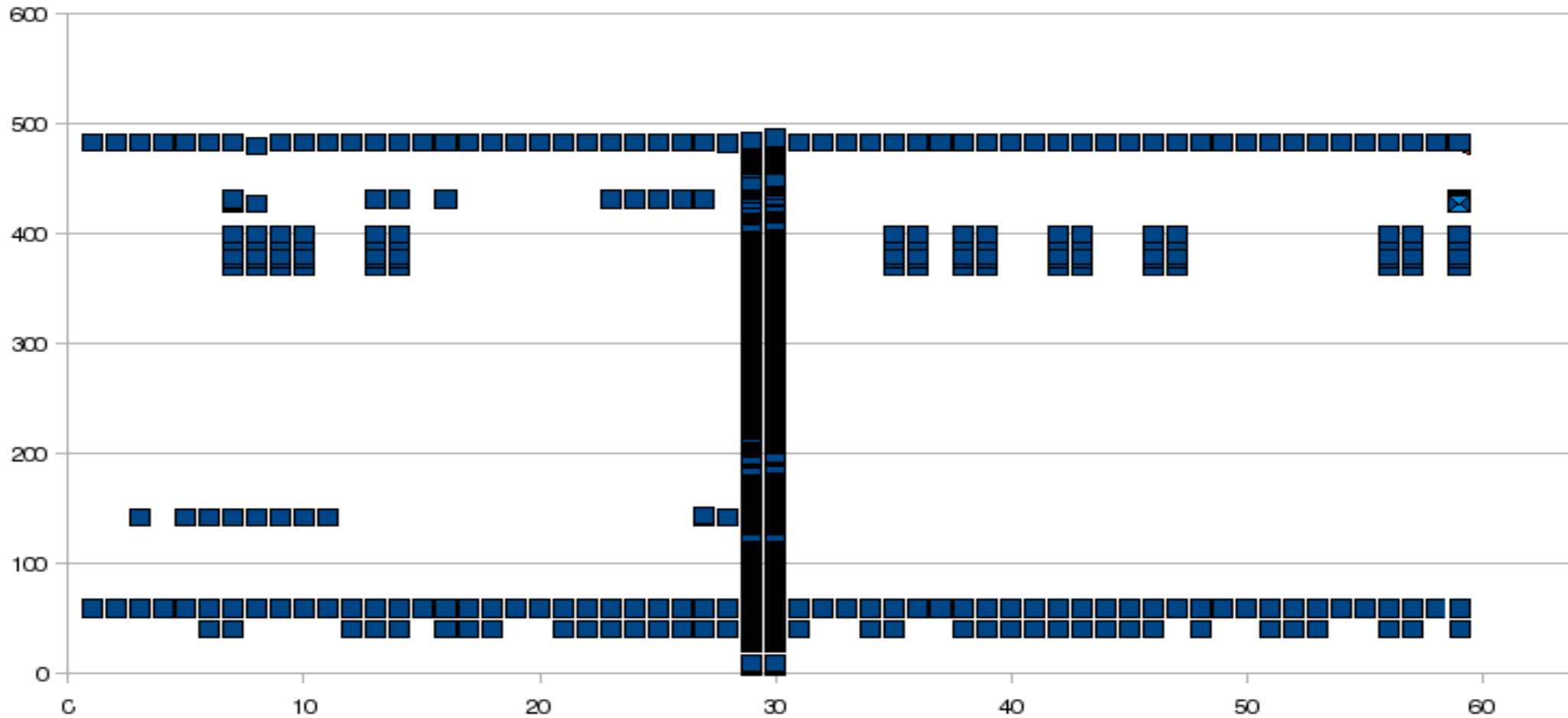
Surface security

file:///2/hi/in_depth/middle_east/2002/conflict_with_iraq/default.stm Amiga Soundtracker Audio

Opis systemu



Opis systemu



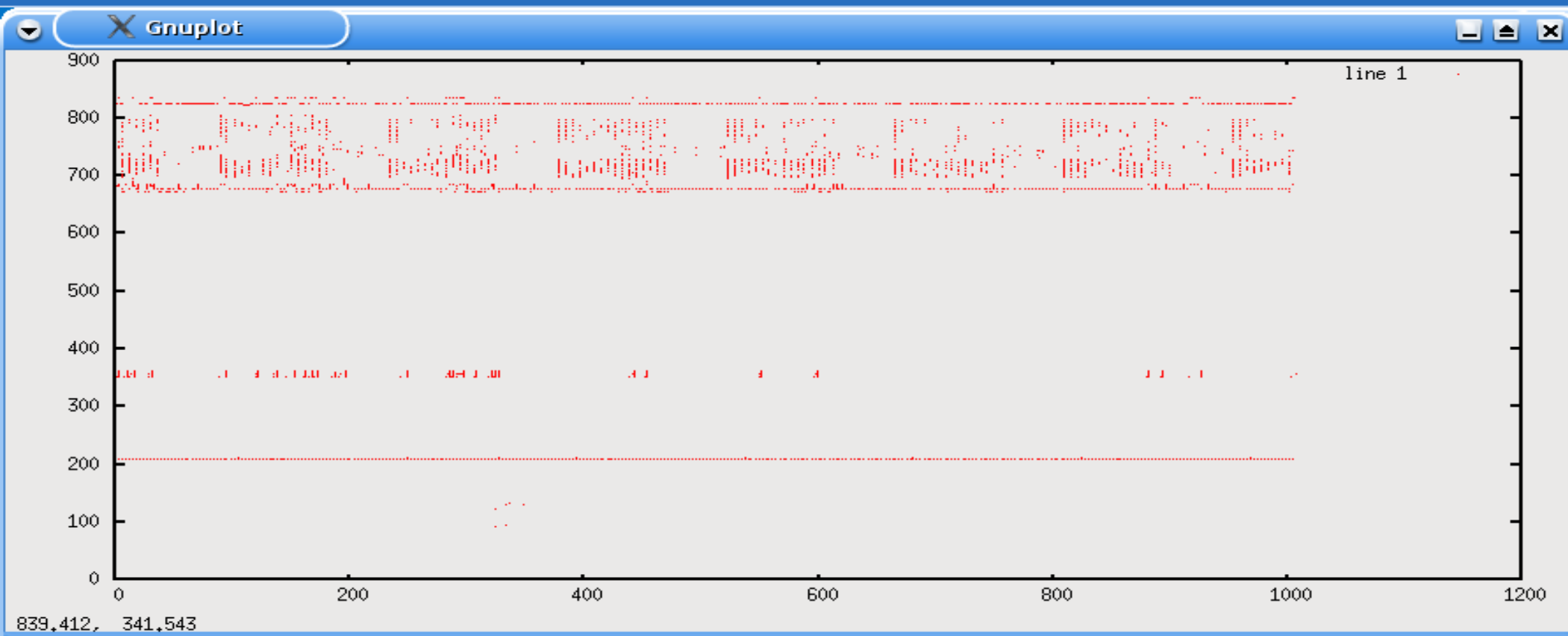
Opis systemu

The screenshot shows a web browser window with the following elements:

- Browser Title Bar:** `http://www.time.com/time/magazine/1998/dom/980302/special_report.clintons_29.html - Konqueror`
- Menu Bar:** Location, Edit, View, Bookmarks, Tools, Settings, Help
- Address Bar:** `http://www.time.com/time/magazine/1998/dom/980302/special_report.clintons_29.html`
- Search Bar:** Google Search
- TIME ONLINE EDITION Logo:** Located at the top left of the page content.
- Article Notice:**

The page you've requested is an excerpt from a book by Brent Scowcroft and George H. W. Bush titled *A World Transformed*, which appeared in the March 2, 1998, issue of *TIME* magazine under the title "Why We Didn't Remove Saddam". **It has been removed from our site** because the publisher did not grant us rights to sell the piece online through the TIME archive.
- Search the TIME Archive:** A search input field, a dropdown menu set to "Articles Since 1985", and a search button.
- Home Page:** A link to "Go to the TIME.com [home page](#)."
- Advertisement:** A "Ford YEAREND CELEBRATION" banner featuring various Ford vehicles and the text "Get the Best Offers during the Biggest Event of the Year, on all Ford vehicles." with a "CLICK TO LEARN MORE" button.
- Status Bar:** `http://ad.doubleclick.net/click;h=v8/3628/3/0/*/l;158576925;0-0;0;17765...ncentives/offers/%3Fbannerid=448880|21271294|158142165 (In new window)`

Opis systemu

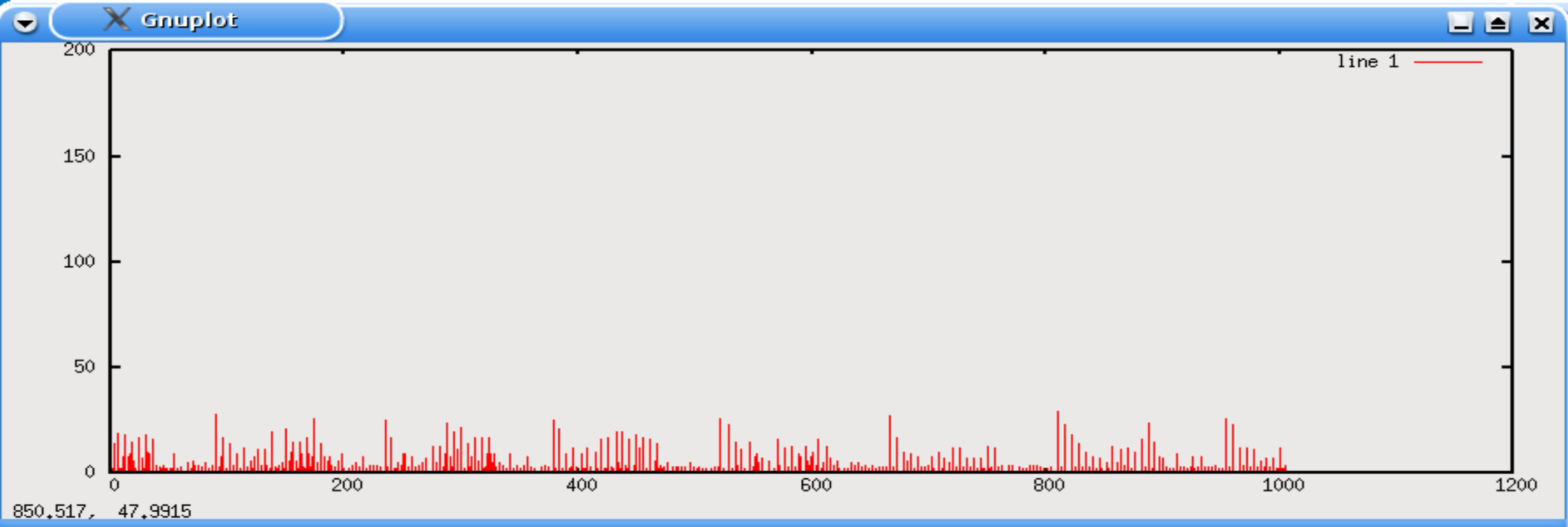


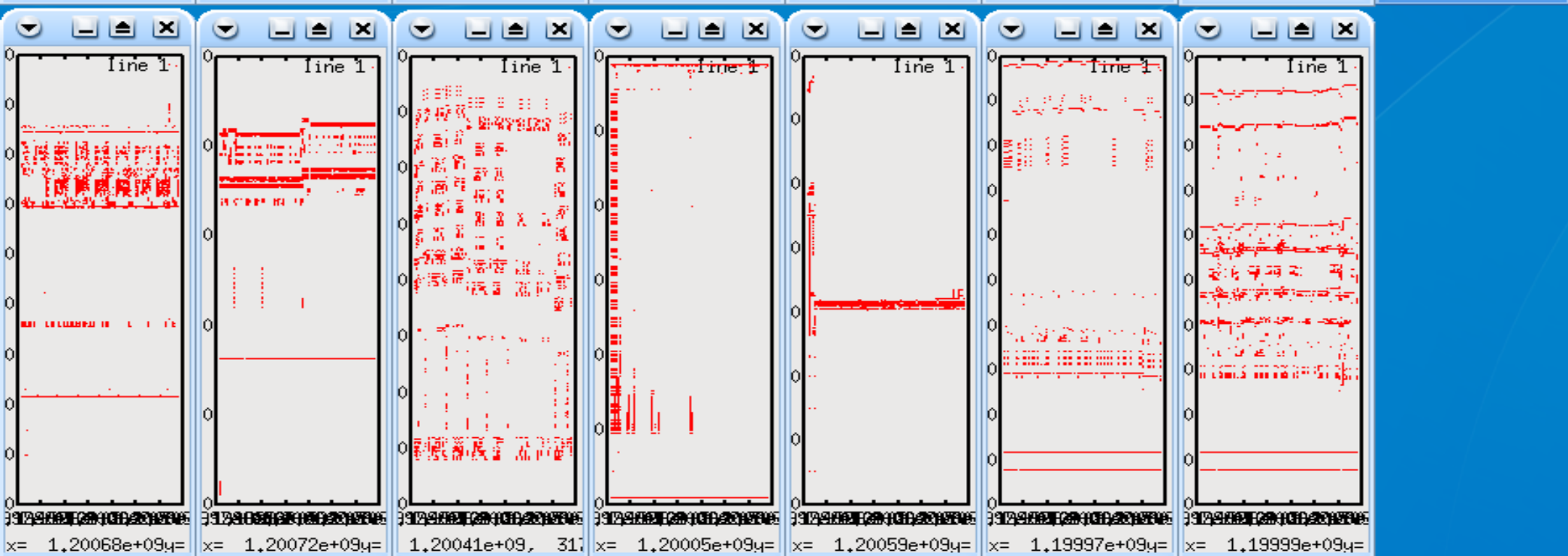
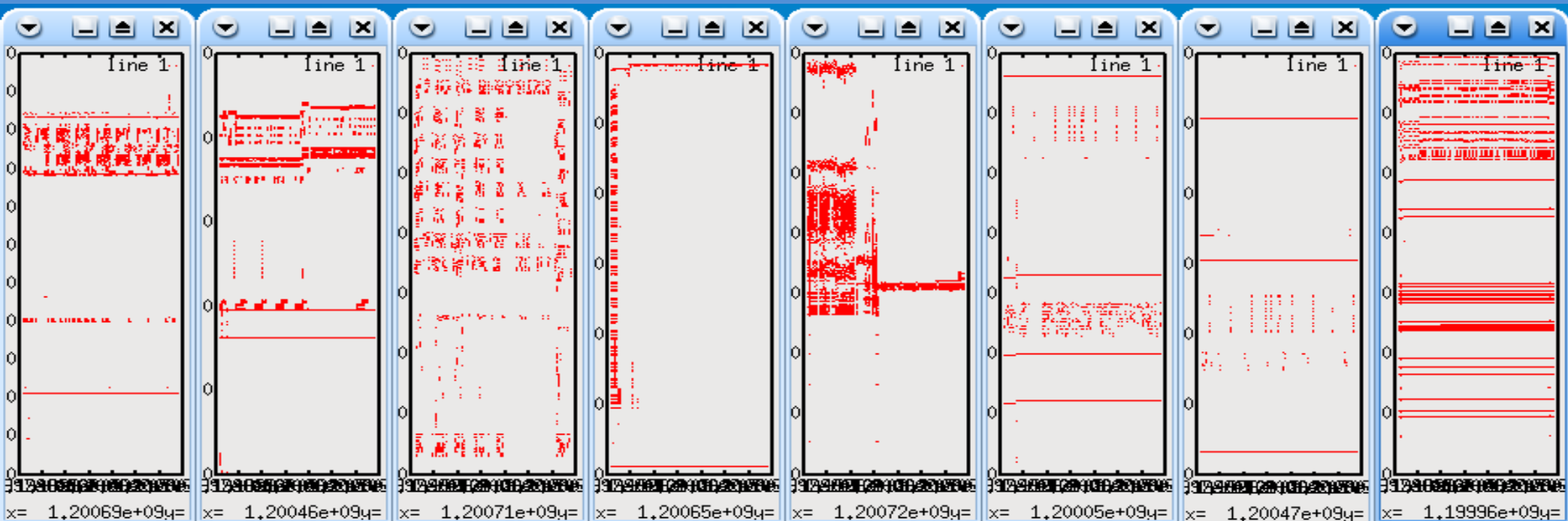
<http://news.bbc.co.uk/2/hi/technology/7149588.stm>

2007-12-18 15:25 -> 2007-12-25 15:16

step: 10 minutes

Opis systemu



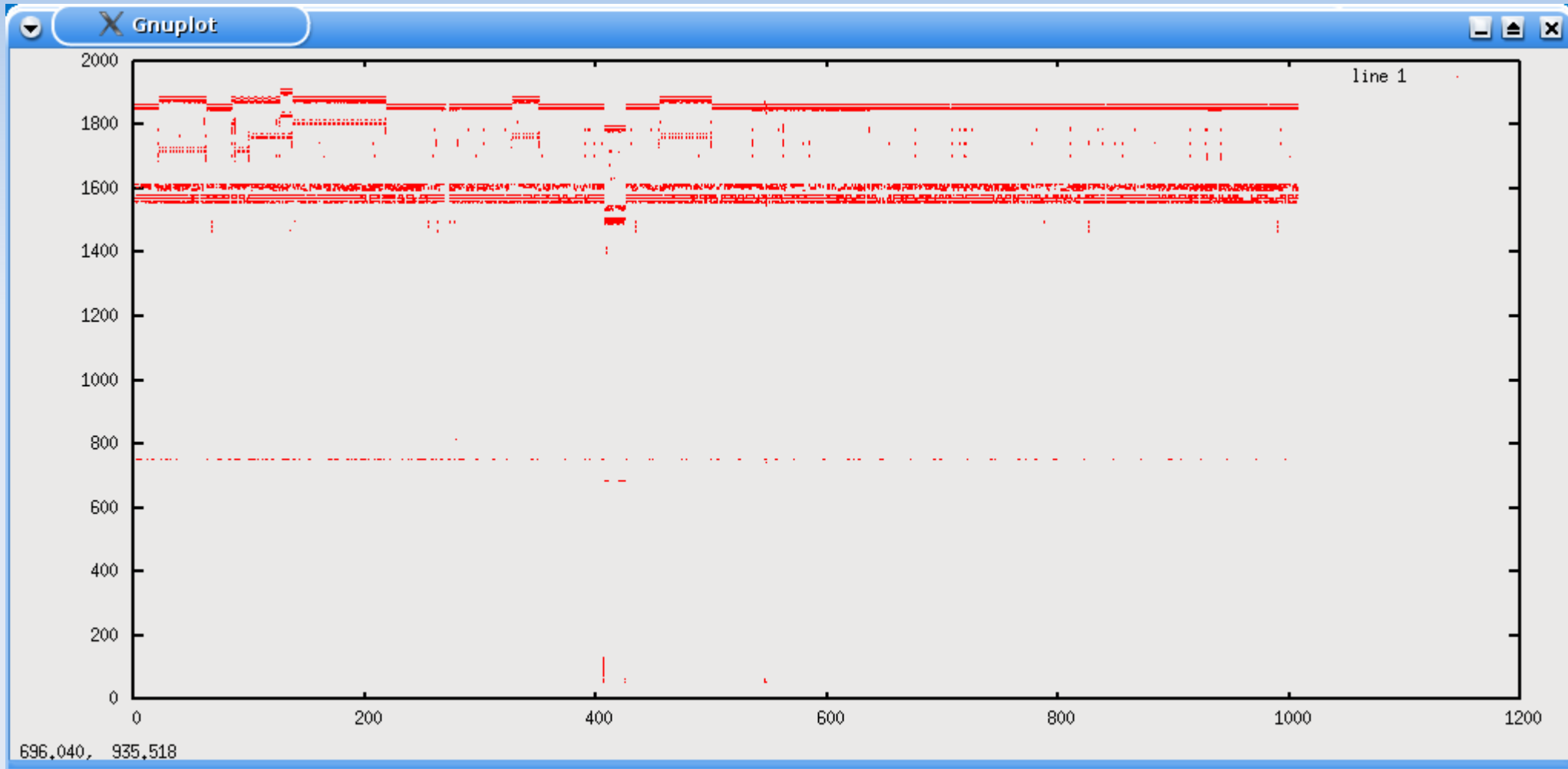


Opis systemu

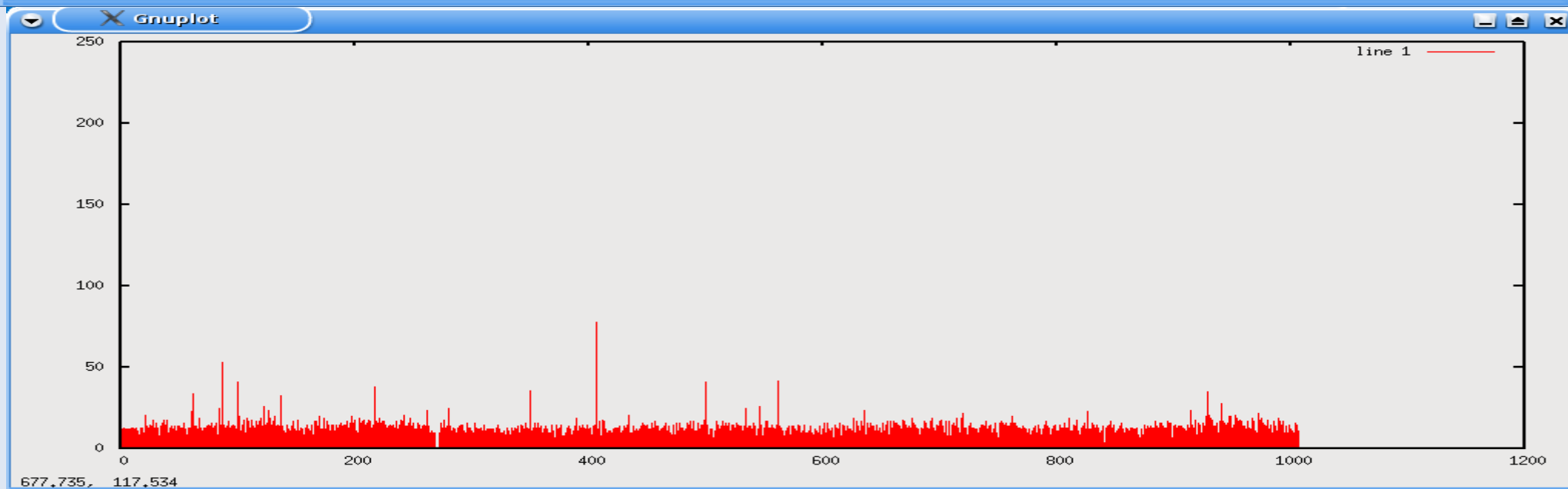
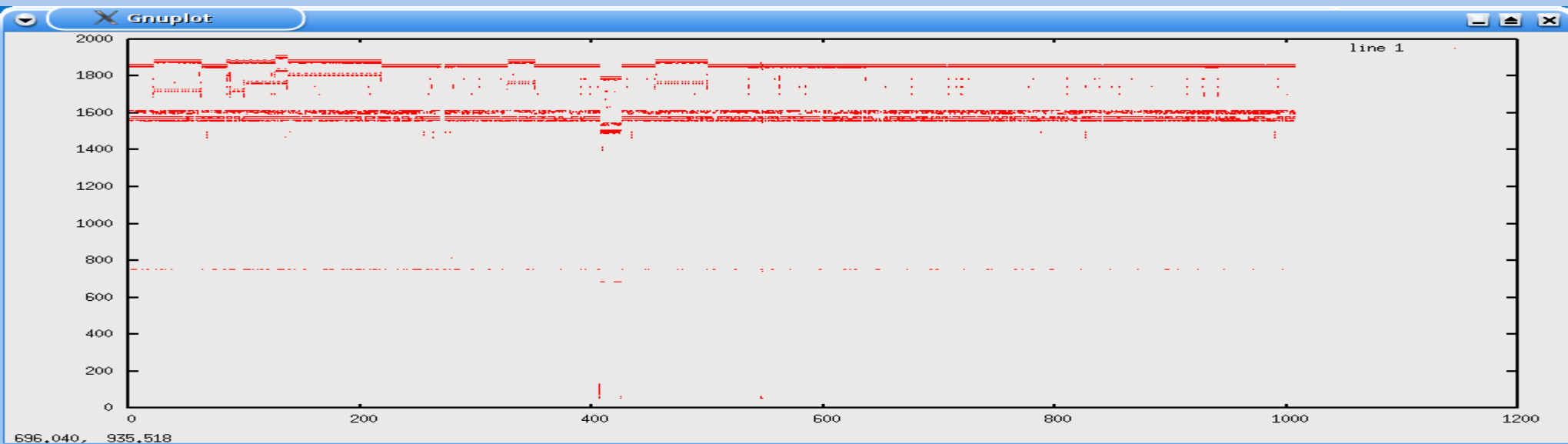
<http://news.bbc.co.uk/2/hi/technology/7149588.stm>

2007-12-18 15:25 -> 2007-12-25 15:16
step: 10 minutes

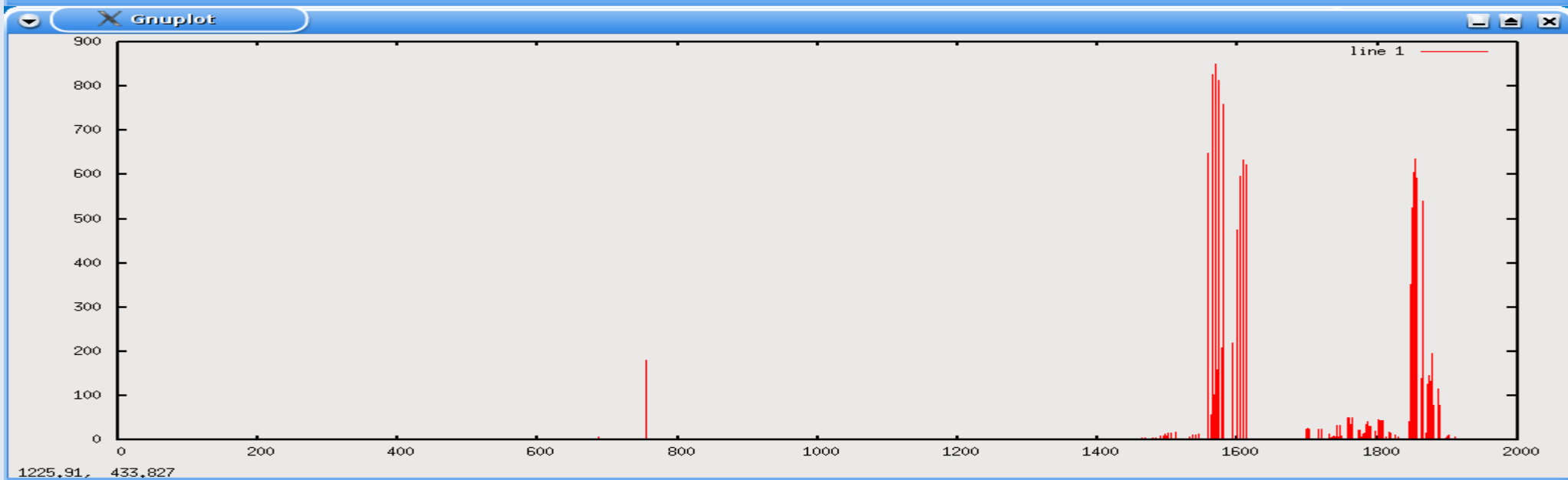
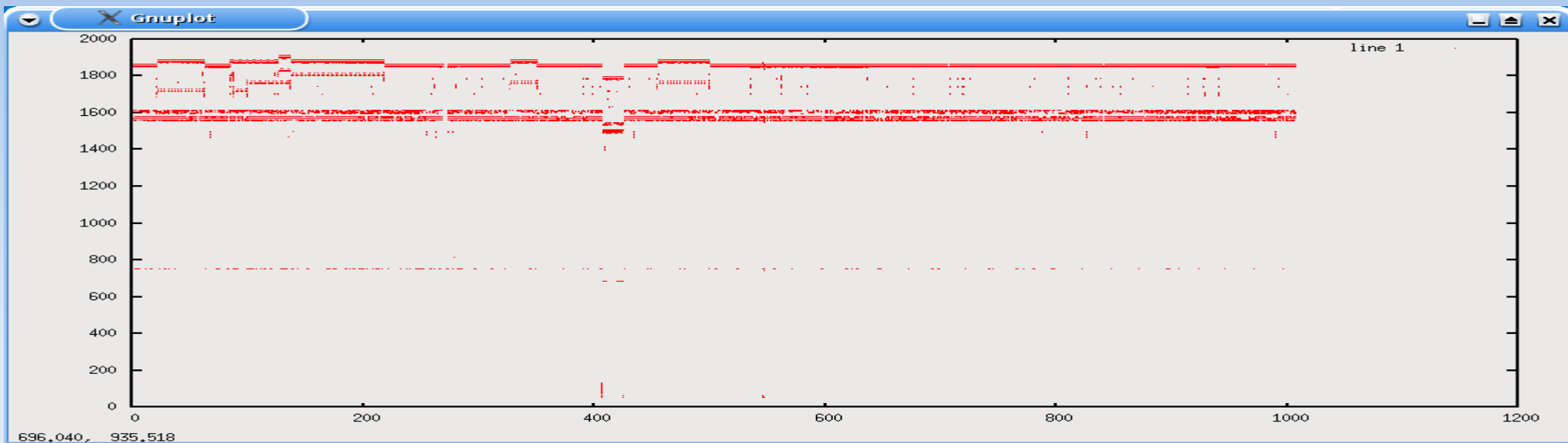
Opis systemu



Opis systemu



Opis systemu



Wykrywanie ataków hackerskich

Opis systemu

Computerworld > French Embassy site for Libya said to be serving malware - Konqueror

Location Edit View Bookmarks Tools Settings Help

http://computerworld.co.nz/news.nsf/scri/7ABECA9FFB080ED5CC2573B3007A6940

Computerworld > French Emba...

Fairfax Business Media | FairfaxBM | Computerworld | PC World | Reseller News | CIO | JobUniverse
Advertise with us - Contact us - Newsletters - Subscribe - Privacy

E-Mail Newsletters

COMPUTERWORLD
The Voice of the ICT Community

RSS

Wednesday, 16 January 2008

Work IT

New Zealand's ICT jobsite

JobUniverse
jobuniverse.co.nz

HOME NEWS TECHNOLOGY SECURITY DEVELOPMENT NETWORK & TELCO SPECIAL MANAGEMENT CAREERS E-TALES FRYUP EVENTS

search here... GO

French Embassy site for Libya said to be serving malware

The French Embassy website for Libya has been compromised and is serving up malware to visitors, according to McAfee.

By Ellen Messmer Framingham | Monday, 17 December, 2007

Email Print

McAfee researcher Francois Paget discovered this on Thursday and the company says it has reported its findings to the French government. The site has been attacked using an [iFrame exploit](#) that inserts an invisible frame in the page in order to re-direct some web browser connections to another location, which serves up a "downloader," code that attempts to reside on the victim machine. If the downloader is successful, the attacker can then remotely attempt to download other malware, "typically a bot or a password-stealing Trojan," says Dave Marcus, McAfee security researcher and communications manager.

Marcus says Paget, a researcher with tools to scan scripts and investigate code behaviour, happened by chance to be looking at the French Embassy website for Libya and discovered the attack code on it. The incident is similar to discoveries made by security researchers of other compromised websites spewing attack code, including that of the [Bank of India](#) and the [MySpace page of Alicia Keys](#).

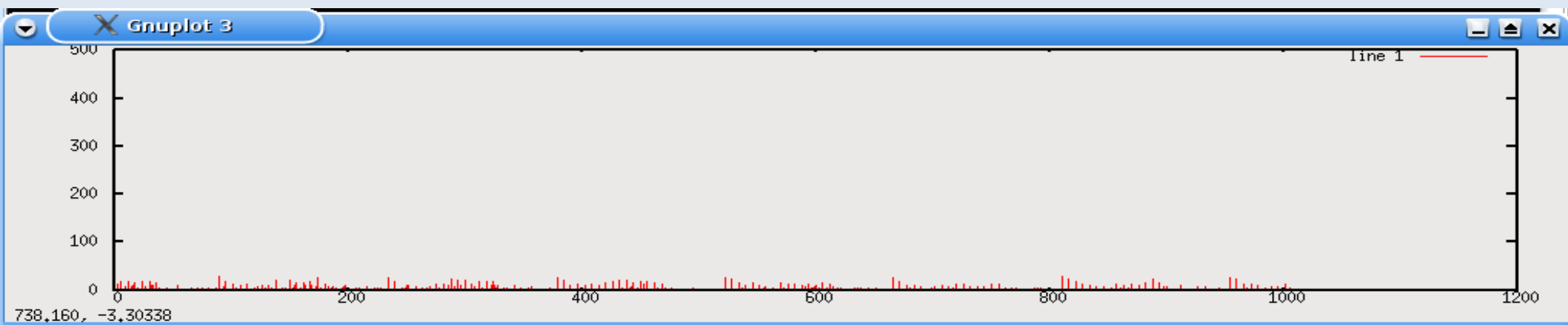
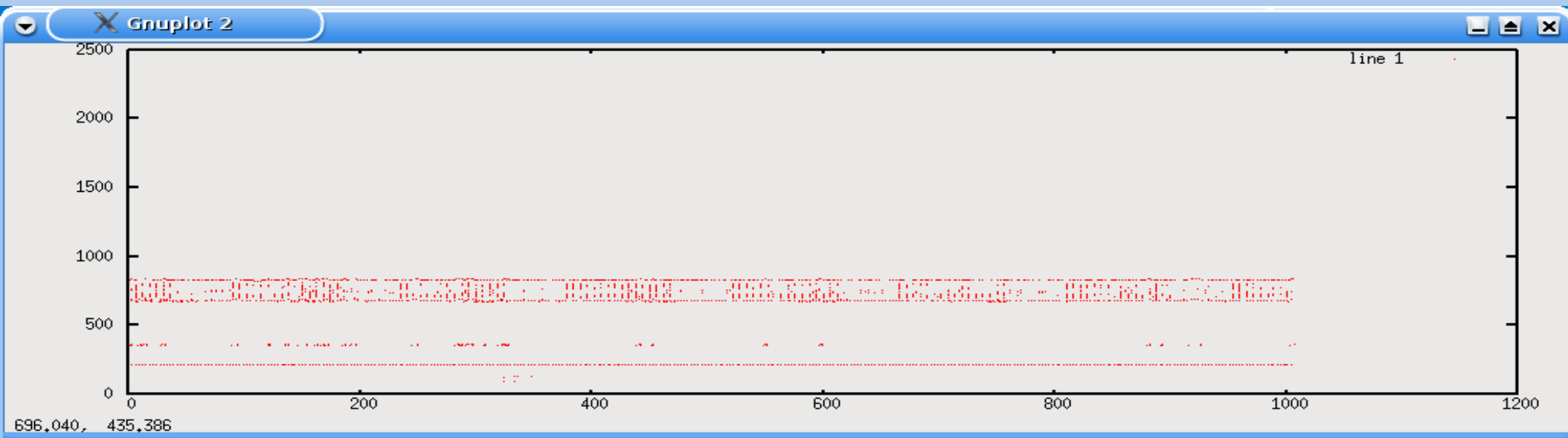
Fairfax Business Media

Click here to subscribe to any of our publications

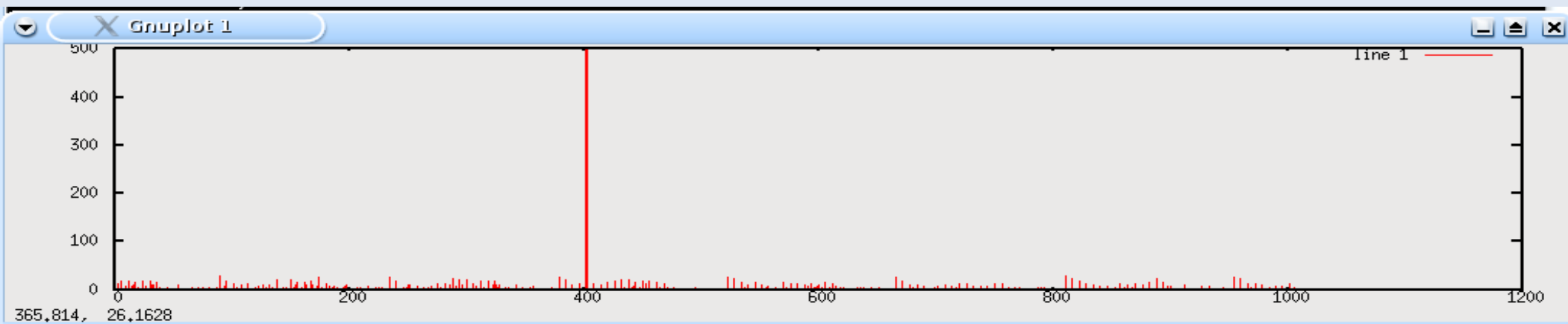
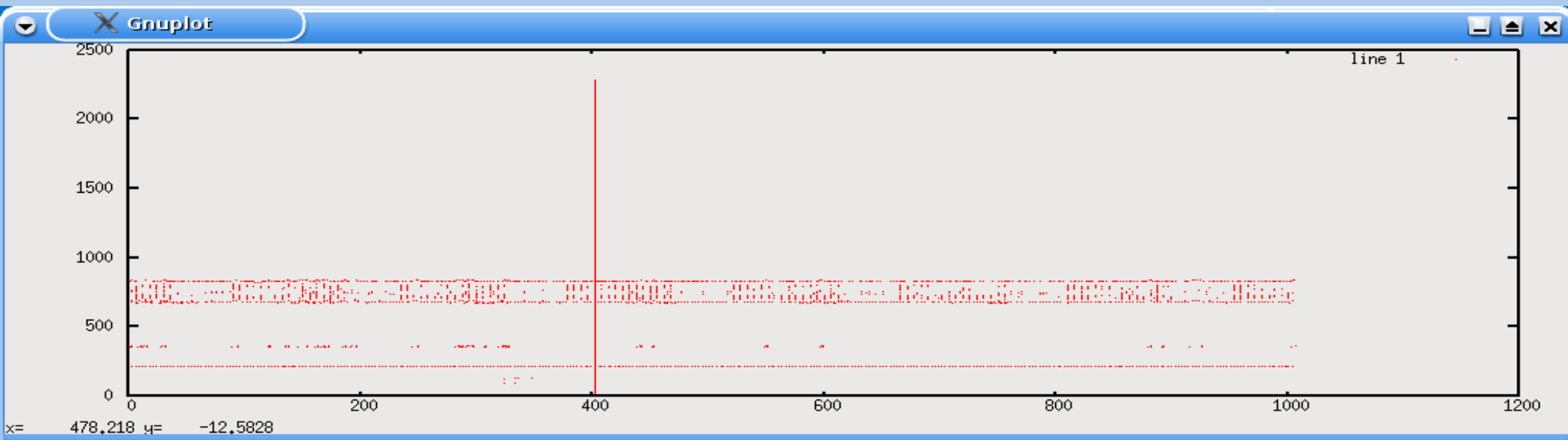
CIO
COMPUTERWORLD
PCWORLD
RESSELLER NEWS

WIN \$15,000 of Product with PC WORLD and hp

Opis systemu



Opis systemu



Sposób zaimplementowania

Prezentacja wideo

Dziękuję za uwagę